CLAIMS

1.- Method based on an algorithm capable of being graphically implemented to be used for the generation or filtering of data sequences and cryptographic applications, comprising the following stages:

a) Defining a cell array distribution with a computer, referenced to a system of coordinates in a vector bidimensional space, provided that the cells in question are capable of adopting two states.

b) definition of a first area within that bidimensional vector space, bordered by a first contour, using part of the said cells to define the successive points of the first contour and including a certain number of those cells in this first area;

c) definition of a second area in that bidimensional space bordered by a second contour using part of the cells to define the subsequent points of the same; this second area contains the first area;

d) choose a cell as the pole, and plot a set of lines from the pole of that cell, and repeat the process, up to a given number of cells which define the second contour, covering all or part of that contour until the first area has been fully swept, using for each line the cells determined by a plotting device such as a Bressenham algorithm; and

e) perform an operation on the contents of each of the cells used when plotting each of the lines of the set and included in that first contour, thereby transforming their state, such as a Logic Xor, each time the cell in question is found in one of the lines of the set.

2.- Method pursuant to the foregoing claim, best described because the bidimensional space in question is materialized in a computer screen and the array distribution of cells is defined by a specific resolution of the screen, which may be selected, and each cell is considered as a pixel or basic element of an image or its analytical representation.

3.- Method as set forth in Claims 1 or 2, characterised in that the second contour matches with the first contour.

4.- Method as set forth in Claims 1 or 2, characterised in that the second contour and the first contour are rectangular and its sides are parallel.

5.- Method as set forth in Claim 2, characterised in that the second contour is the border of the graphic screen or an analytical representation of the same.

6.- Method, as set forth in Claim 1, characterised in that the pole is located within the area enclosed by the second contour.

7.- Method, as set forth in Claim 6, characterised in that the pole in question is located in a cell next to one of the two contours.

8.- Method, as set forth in Claim 1, characterised in that the second contour is unregularized and the cells of the same are obtained by means of a Pseudo-Noise Sequence Generator (PNSG), so that the distance from the cells within that second

contour to their corresponding pole is dependent on the output of the Pseudo-Noise Sequence Generator.

9.- Method, as set forth in Claim 1, characterised in that the distance from the pole to the origin of the reference coordinates is obtained by means of Pseudo-Noise Sequence Generator (PNSG), so that the distance in question is dependent on the output of the Pseudo-Noise Sequence Generator.

10.- Method, as set forth in Claim 1, characterised in that it likewise includes a stage d1) prior to e) which consists in assigning the successive values of a data block with a certain length, or undetermined, to be encrypted or filtered, associating them in a pre-arranged manner to the cells of the said array delimited by the first contour and in that the extraction of data obtained by the application of this method is likewise carried out by means of an appropriate association to the cells in question in a pre-established manner.

11.- Method, as set forth in Claim 10, characterised in that the prearranged association of data to the cells in question is made in order, row by row.

12.- Method, as set forth in Claim 10, characterised in that the prearranged association of data to the cells in question is made in order, column by column.

13.- Method, as set forth in Claim 10, characterised in that the foregoing prearranged association of data to the cells is made in radial order starting from a pole with the precaution of not overlapping data so that such data only occupies positions not yet occupied in the array of cells to be filled in.

14.- Method, as set forth in Claim 10, characterised in that the foregoing prearranged association of data to the cells is undertaken pursuant to any of the Claims 11 to 13, and its extraction or reading is made according to any of the procedures set out in Claims 11 to 13.

15.- Method, as set forth in Claims 10 to 14, characterised in that the data block to be ciphered is made of a sequence stream generated by a Linear Feedback Shifted Register (LFSR).

16.- Method, as set forth in Claim 10, characterised in that stages a),b),c),d),d1 and e) are repeated a certain number of times at will, and each time any of the following variants may be applied:

- choice of different poles;
- change of contour size or form, or relative distance and position between the first and second contours in question; and
- undertaking a specific number of complete or incomplete rotations of the second contour, or plotting the set of lines originating from the pole and based on the cells from the second contour.

17.- Method for the encryption and decryption of messages relayed between a first and second station, or between multiple stations, consisting in variable length binary data blocks, and using the same graphic or analytic algorithm both for encryption and decryption as set out in Claims 10 to 16,

the data being introduced in an array delimited by the first contour and because the operation, made on the contents of a cell each time this cell of the first contour is used to plot a line of the set, makes use of the value stored in such cell and its corresponding value in a pseudo-random linear sequence generator, and the correlation is established pursuant to a specific order in the data array of the first contour, and if the data introduced, completely fills the array in question, the additional data is assigned, defining new pairs of first and second contours, being the first of these a new array for the loading of plaindata. And so on, until plaindata is off.

18.- Method for encryption and decryption, as set forth in Claim 17, characterised in that the values of the pseudo-randomly generated linear sequence, for example, by a linear feedback shifted register (LFSR) of n degree, are filtered by any of the methods provided under Claims 10 to 16, operating as a non-linear filtering method.

19.- Method, as set forth in Claim 18, characterised in that it includes a secret key, randomly generated to be exchanged by means of a secure server between the sender(s) and recipient(s), the said key being the same for the encryption and decryption process, the contents of such key comprise the definition of the Linear Feedback Shifted Register, as well as the coordinates of the pole, the array size, the distance from the first contour to the second one, and any other parameter which may be required for any of the specific implementations foreseen under any of the methods set forth in Claims 10 to 16.

20.- Method as set forth in Claim 19, characterised in that the Linear Feedback Shifted Register (LFSR), is defined by a binary coefficient polynomial and a seed or initial state of the LFSR apt for the generation of a periodic sequence.

21.- Method, as set forth in Claim 17, characterised in that the cell content is any type of digital data subject to

being handled, treated or stored individually as a bit, byte, nibble, word, double word, and the number of possible states of the cells includes all the possibilities which are specific to the nature of the type of data in question, or at least some of them.

22.- Method, as set forth in Claim 21, characterised in that the contents of each cell are data bits and those cells are subject to undergoing at least two states.

23.- Method, as set forth in Claim 21, characterised in that each cell content is a byte of data, those cells being capable of undergoing at least 256 states.

24.- Method, as set forth in Claim 17, characterised in that the size of both contours or data array and the polar coordinates and any other parameter required are obtained by means of pseudo-random sequence generator (i.e. LFSR with a primitive polynomial, non linear filtered LFSR, etc.).

25.- Method, as set forth in Claim 24, characterised in that the said (LFSR) includes a binary seed of degree 63 and a primitive polynomial of degree 63.

26.- Method based on an algorithm subject to being implemented in a graphic manner for the generation or filtering of data sequences and cryptographic applications, which encompasses the following stages:

a) Defining a cell array distribution with a computer referenced to a system of coordinates in a vector space, which is at least three-dimensional, and whose cells are capable of adopting at least two states.

b) Defining within that first space, which is at least three-dimensional, a first area, defined by a first encircling surface using part of those cells in order to define the subsequent points of the first encircling surface, and

containing this first encircling surface a certain number of those cells.

c) Defining within that vector space, which is at least three-dimensional, a second area, bordered by a second encircling surface, using part of those cells to define the subsequent points of that encircling surface, whose second encircling surface includes the first encircling surface.

d) choose a cell as a pole and plot a set of lines from the same successively up to a certain number of cells which define the second encircling surface, covering part or all of the same until the first surface has been fully swept, using for each line a number of cells determined by a plotting technique similar to a Bressenham algorithm; and

e) perform on the contents of each of the cells used to plot each of the lines of the set and included within the first encircling surface an operation which transforms their state, such as a Logic Xor, as many times as that cell is found in one of the lines of the set.

27.- Method based on an algorithm subject to being implemented graphically, for the generation or filtering of data sequences or cryptographic applications, which encompasses the following stages;

a) Defining a cell array distribution with a computer referenced to a system of coordinates in a vector space, which is at least three-dimensional, and whose cells are capable of adopting at least two states.

b) Defining a first area, within that first space, which is at least three-dimensional, defined by a first encircling surface using part of those cells in order to define the subsequent points of the first encircling surface, and containing this first encircling surface a certain number of those cells.

c) Defining a second area within that vector space, which is at least three-dimensional, bordered by a second encircling surface, using part of those cells to define the subsequent points of that encircling surface, whose second encircling surface includes the first encircling surface.

d) draw a line by means of any plotting technique, similar to a Bressenham algorithm, comprising a certain number of cells and plot a cluster of planes stemming from that line, the said line being the axis of the cluster, and each plane extending from the line in question to a certain number of cells which define the second encircling surface, covering part or the whole of this second encircling surface until the first surface has been fully swept; and

e) perform on the contents of each of the cells used to plot each of the planes of the set and included within the first encircling surface an operation which transforms their state, such as a Logic Xor, as many times as that cell is found in one of the planes of the set.

28.- Method based on an algorithm subject to being implemented graphically for the generation or filtering of data sequences and cryptographic applications, comprising the following stages:

a) Defining a cell array distribution with a computer referenced to a system of coordinates in a unidimensional vector space, whose cells are capable of adopting at least two states;

b) define in this unidimensional vector space a first segment, bounded by two points;

c) define in this unidimensional space a second segment likewise bounded by two points; this second segment contains the first one; we consider that all inside points of the second segment provide the outline of its contour;

d) choose a cell as a pole and plot from the same a set of lines from that pole, successively, linking all or part of the cells which define the second contour, and covering all or part of that contour until the first segment has been fully swept; and

e) perform an operation on the contents of each of the cells used when tracing the lines within of the set, and included in that first segment, in order to modify their state, such as an logic Xor, each time the cell in question is found in one of the lines of the set.

29.- Method set forth under Claims 26, or 27, characterized in that apart from including a preliminary phase d1) before e) which consists in assigning the subsequent values of a data block whether of definite or indeterminate length, to be encrypted, or filtered, associating them in a prearranged manner to the cells of that array delimited by the first encircling perimeter in question, and in that the operation to extract data following the application of this method is also conducted by means of a prearranged association, as may be appropriate.

30.- Method set forth under Claim 28, characterised in that it likewise includes a preliminary phase d1) prior to e) which consists in assigning the subsequent values of a data block whether of definite or indeterminate length, to be encrypted, or filtered, associating them in a prearranged manner to the cells of that array delimited by the first segment, and in that the operation of data extraction following the application of this method is also conducted by means of a prearranged association, as may be appropriate.

31.- A computer programme directly loaded in the memory of a computer including parts of the programming code to perform stages set out in Claims 1 to 3,6 to 14, and 16 to 28 when the said programme is executed in that computer.